State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0051 Network Perimeter Security Policy	
Subject: This policy defines DES network perimeter security requirements.	***Effective Date:*** **05/02/03**	***Revision:*** 1.1

1. Summary of Policy Changes

1.1. 01/07/05 - The 11/22/04 major rewrite by DTS staff was implemented on 01/07/05

2. Purpose

2.1. This DES Network Perimeter Security Policy specifies the minimum risk mitigation requirements for the exposure to the Internet of sensitive information and information systems supporting Department of Economic Security (DES) assets.

2.2. This policy establishes minimum security requirements for the use of the Internet network by DES. This policy is written to ensure that adequate measures are in place to protect DES systems and data from intruders, file tampering, break in, and service disruption.

2.3. The objective is to comply with the State of Arizona guidelines to maintain a proper level of network security, specifically regarding connectivity to the Internet, commensurate with risk and threat assessment. The Department policy states that a firewall interposed between the Internet and the DES business network must be used for ensuring the proper protection of the sensitive information, network, or system.

3. Scope

3.1. This policy applies to all DES administrative entities, councils, divisions, administrations, and programs.

3.2. This policy applies to all PC's, laptops, workstations, servers, and any other network devices connected to the DES wide area network or local area networks.

3.3. This policy applies to all employees, full-time, part-time, or temporary; contractors, and other governmental and non-governmental entity staff that are connected to the DES network.

4. Responsibilities

4.1. The **DES Director, Deputy Directors, Associate Directors, and Assistant Directors** are responsible for implementing and enforcing this policy.

4.2. The **DES CIO and the Division of Technology Services** are responsible for implementing this policy.

4.3. **Chief Information Security Officer (CISO)** is responsible for:

4.3.1. Providing counsel and recommendations about DES security policies, standards, and procedures to the DES CIO and all interested parties.

4.3.2. Coordinating, and interpreting DES IT security policy

4.3.3. Deciding when to shutdown the DES network to protect sensitive and proprietary information and to protect the integrity of the DES network, in the case of a cyber attack.

4.3.4. Chairing the Security Planning Team.

4.3.5. Overseeing the development and implementation of an overall network security plan for DES systems.

4.3.6. Issuing operational information and documents about security policy, standards, guidelines and procedures.

4.3.7. Providing oversight for DES network security.

4.3.8. Reporting the effectiveness of DES security policies, standards, procedures, and guidelines.

4.4. **Security Planning Team (SPT)** is responsible for:

4.4.1. The development of DES IT security policies and plans that affect the entire Agency.

4.4.2. Coordinating the IT security program and all activities designed to protect IT resources.

4.4.3. Reporting the effectiveness of DES IT security activities to the DES CIO and CISO.

5. Definitions and Abbreviations

5.1. Definitions

5.1.1. **Ssh** –Secure shell. An encrypted alternative to telnet.

5.1.2. **Dual-homed server** – a server that has multiple network adapters (virtual or physical) defined and enabled where each network adapter is defined to route traffic for a differing range of IP addresses. By their very nature almost all firewalls are, at a minimum, dual-homed.

5.1.3. **FTP** – File Transfer Protocol is a standard Internet protocol, is the simplest way to exchange files between computers on the Internet.

5.1.4. **Telnet** – A way you can access someone else's computer, assuming they have given you permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers.

5.1.5. **TN3270** – TN3270 is a subset of the Telnet protocol, allowing remote computers running TCP/IP to emulate IBM 327x mainframe display terminals, typically used to access IBM Mainframes. Other variants based on the Telnet protocol include TN5250 used typically to communicate with IBM S series (s/34, s/36, s/38) mini-computers and AS400s and TN3287 to emulate printers attached to an IBM mainframe.

5.1.6. **Rlogin** – Remote login is a command that allows an authorized user to login to other machines (hosts) on a network and to interact as if the user were physically at the host computer.

5.1.7. **HTTP** – The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

5.1.8. **SSL** – Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.

5.1.9. **POP3/IMAP** – POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netscape and Microsoft Internet Explorer browsers. An alternative protocol is Internet Message Access Protocol (IMAP). With IMAP, you view your e-mail at the server as though it was on your client computer. An e-mail message deleted locally is still on the server. E-mail can be kept on and searched at the server. POP can be thought of as a "store-and-forward" service. IMAP can be thought of as a remote file server.

5.1.10. **NNTP** – Network News Transport Protocol is a standard protocol that specifies a method for posting, distributing, searching and archiving news articles on the Internet.

5.1.11. **Lp Services** – Line Printer spooler commands.

5.1.12. **finger** – A program that tells you the name associated with an e-mail address.

5.1.13. **gopher** – From about 1992 through 1996, Gopher was an Internet application in which hierarchically-organized text files could be brought from servers all over the world to a viewer on your computer. Especially in universities, Gopher was a step toward the World Wide Web's Hypertext Transfer Protocol (HTTP), which effectively replaced it within a short time.

5.1.14. **whois** – A program that will tell you the owner of any second-level domain name who has registered it with Verisign (or with Network Solutions, which was acquired by Verisign).

5.1.15. **SQL** – Structured Query Language is a standard interactive and programming language for getting information from and updating a database.

5.1.16. **Rsh** – A UNIX command often used for remote system administration.

5.1.17. **Citrix** – A company that markets thin client and VPN software products.

5.1.18. **NFS** – The Network File System is a client/server application that lets a computer user view and optionally store and update files on a remote computer as though they were on the user's own computer. NFS was developed by Sun Microsystems and has been designated a file server standard.

5.1.19. **VPN**- A Virtual Private Network is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

5.2. **Abbreviations**

5.2.1. **CIO** – **C**hief **I**nformation **O**fficer

5.2.2. **DES** – **D**epartment of **E**conomic **S**ecurity

5.2.3. **DDD** – **D**ivision of **D**evelopmental **D**isabilities

5.2.4. **DMZ** – **Dem**ilitarized **Z**one

5.2.5. **DOA** – **D**epartment **o**f **A**dministration

5.2.6. **DNS** – **D**omain **N**ame **S**erver

5.2.7. **CISO** – **C**hief **I**nformation **S**ecurity **O**fficer

5.2.8. **ISA** – **I**nformation **S**ecurity **A**dministration

5.2.9. **DTS** – **D**ivision of **T**echnology **S**ervices

Abbreviations (continued)

5.2.5 **GITA** – **G**overnment **I**nformation **T**echnology **A**gency

5.2.6. **IT** – **I**nformation **T**echnology

5.2.7. **NC** – **N**etwork **C**omputer

5.2.8. **PC** – **P**ersonal **C**omputer

5.2.9. **SIPC** – **S**tatewide **I**nfrastructure **P**rotection **C**enter

5.2.10. **SPT** – **S**ecurity **P**lanning **T**eam

6. POLICY

6.1. General

6.1.1. The responsibility for protecting DES resources from the Internet is the responsibility of all DES employees. This policy also applies to contractors and other governmental and non-governmental entities that are provided network access by DES.

6.1.2. Employees will access the Internet only through trusted DES Internet access points. Any form of communication to or from workstations outside the internal (trusted) network is strictly prohibited without review and authorization of the DES Information Security Administration (ISA). This includes modems, leased lines to other networks, etc.

6.1.3. All users who require access to Internet services must do so by using DES approved software and Internet gateways.

6.1.4. The basic DES policy for security strategy on the Internet is to deny any service that is not expressly permitted, inbound to DES as well as outbound.

6.1.5. The details of the DES internal trusted network should not be visible from outside the firewall.

6.2. **Firewall** - The firewall will be configured using Industry “best practices” including but not limited to the following:

6.2.1. The DES will use a robust “Firewall System” interposed between the Internet and the DES business network. All Internet traffic from inside to outside, and vice-versa, must pass through the firewall implementation.

6.2.2. Access from the Internet to the DES public information systems must not make sensitive information or information systems vulnerable to compromise.

6.2.3. All services and traffic to be authorized across the firewall implementation must be well documented. The business need, protocol used, inbound and/or outbound, port assignments, known vulnerabilities, and risk mitigation statements will all be documented.

6.2.4. Only network sessions using strong authentication and encryption will be permitted to pass from the Internet to inside through the firewall implementation. Where users are required to access internal systems and networks from, or across, the Internet, end-to-end encryption and strong authentication controlled by a DES organization will be employed.

6.2.5. The firewall must be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse.

6.2.6. The firewall will notify the firewall administrator(s), in near real-time of any item that may need immediate attention such as an attempted break-in to the network, limited disk space available, or other messages, so that action may be taken. The DES Incident Handling procedure will be followed at this point in an incident.

6.2.7. The firewall software is run on a dedicated computer; all non-firewall related software, such as compilers, editors, communications software, etc., will be deleted or disabled.

6.2.8. In the event of a firewall failure, all firewalls will fail to a configuration that denies all services, and require a firewall administrator(s) to re-enable services.

6.2.9. Source routing must be disabled on all firewalls and external routers.

6.2.10. The firewall must not accept traffic on its external interfaces that appear to be coming from internal network addresses.

6.2.11. The firewall must provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.

6.2.12. Secure media must be used to store log reports such that access to this media is restricted to only authorized personnel.

6.2.13. Firewalls must be tested off-line and the proper configuration verified. "Test" firewalls must be provided for this purpose.

6.2.14. Appropriate firewall documentation must be maintained on off-line storage at all times. Such information must include but not be limited to the network diagram, including all IP addresses of all network devices, the IP addresses of relevant hosts of the Internet Service Provider (ISP) such as external news server, router, DNS server, etc. and all other configuration parameters such as packet filter rules, etc. Such documentation must be updated any time the firewall configuration is changed.

6.2.15. The DES SWG and firewall administrator(s) must review the network security policy and maintenance procedures on a regular basis (every three months minimum). If requirements for network connections and services have changed, the security policy must be updated and approved.

6.2.16. The firewall implementation (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files must be locked up so that the media is only accessible to the appropriate personnel.

6.2.17. Only the firewall administrator(s) will have privileges for updating system executables or other system software. Any modification of the firewall component software must be done by a firewall administrator(s) and requires the approval of the DES CIO.

6.2.18. The firewall administrator(s) must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.

6.2.19. If application-level proxy firewalls are used, out-bound network traffic should appear as if the traffic had originated from the firewall (i.e. only the firewall is visible to outside networks).

6.3. Host Based Security

6.3.1. Host-based security will be the primary method of protecting DES systems. This Internet security policy in no way abrogates the responsibilities of users, system managers, system owners, or administrators to protect sensitive data and systems.

Host-based security will include, but is not limited to: host-based intrusion detection and/or security baseline install checklists.

6.4. **Demilitarized Zone (DMZ)**

6.4.1. Public Internet servers must be placed on subnets separate from internal Company networks. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

6.5. **Network Information Dissemination**

6.5.1. Information regarding access to, or configuration of, DES computer and communication systems, such as dial-up modem phone numbers or network diagrams, are considered confidential. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or made available to third parties without the written permission of the DES ISA.

6.5.2. ISA will direct periodical scanning of direct dial-in lines to monitor compliance with policies.

6.6. **Firewall/Router Event Logging**

6.6.1. When possible and practical, dedicated log servers should be located behind a secure portal (firewall) for capturing log data from the firewalls themselves. The rationale for this is once a machine has been compromised, the hacker will usually attempt to disable or destroy any logs on the compromised machine.

6.7. **Firewall Architecture**

6.7.1. All in-bound Internet services must be processed by proxy software or state-full inspection at the firewall. If a new service is requested, that service will not be made available until a proxy is available from the firewall vendor and tested by the firewall administrator(s). A custom proxy can be developed in-house or by other vendors only when approved by the DES CIO and CISO.

6.7.2. DES must run an external DNS for externally available machines only, and a separate internal DNS for internal only machines that can refer to and external machine.

6.7.3. To reduce the vulnerability of protocol-based attacks, firewall implementations must use technologies capable of access control decisions based on information examined as high as the application layer. That is, application proxy or state-full aware technologies. Simple packet filtering or circuit-level firewall implementation will not be implemented as the only (sole) method of protecting internal resources from external (unauthorized) access. It must be used in conjunction with other industry accepted protection methods, such as application proxying...

6.8. **Network Trust Relationships**

6.8.1. All connections from the DES network to external networks must be approved by the CISO and Technical Services. Whenever possible external networks will be reviewed to verify that they have acceptable security controls and procedures. All connections to approved external networks will pass through DES approved firewalls.

6.8.2. The ISA will ask functional managers to validate the need for all such connections on an annual basis. When an IT unit is notified by the ISA that the need for the connection to a particular network is no longer valid, all accounts and parameters related to the connection must be deleted within two working days.

6.9. **Virtual Private Networks (VPN)**

6.9.1. Any connection between private and public or un-trusted networks must use encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network. All "peer to peer" VPN connections must be approved by the DES CIO, CISO, and Technical Services, prior to implementation.

6.9.2. All connections between clients to services or applications located behind the firewall within The DES trusted network, that are over un-trusted public networks must use encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network. Such connections will be considered extensions of The DES trusted network, and as such do not fall under the service restrictions that follow.

6.10. **Service Specific Policies**

6.10.1. The table in Attachment A contains examples of some of the most common services that need to be approved by the Security Working Group before implementation. It is not an all-inclusive list and is subject to change.

7. **Implications**

7.1. All DES access to and from the Web must occur from/to servers located in the Centralized DES DMZ.

8. **Implementation Strategy**

8.1. This policy requires immediate DES-wide implementation, pending the availability of required funding.

9. **References**

9.1. Several pending DES IT Standards documents will be added here when they are adopted.

10. **Attachments**

10.1 Attachment A – Service Specific Policies

11. **Associated GITA IT Standards or Policies**

11.1 P800 - IT Security Policy

11.2 P800-S805 - Risk Management Standard

11.3 P800-S810 - Account Management Standard

11.4 P800-S820 - Authentication and Directory Services

11.5 P800-S825 - Session Controls Standard

11.6 P800-S830 - Network Security Standard

11.7 P800-S850 - Encryption Technologies Standard

11.8 P800-S855 - Incident Response and Reporting Standard

11.9 P800-S860 - Virus and Malicious Code Protection Standard

11.10 State of Arizona Target Security Architecture IT Technical Document

12. **Review Date**

12.1. This document will be reviewed twelve (12) months from the original adoption date and every twelve months thereafter.

Attachment A – Service Specific Policies

Service	Policy				Policy
	Inside to Outside		Outside to Inside		
	Status[1]	Auth[2]	Status[1]	Auth[2]	
Ssh	Yes	No	No	No	Allow outbound ssh instead of telnet.
FTP	Yes	No	No	No	FTP access will be allowed from the internal network to the external. For transmission of sensitive information, VPN's should be implemented. No FTP access will be allowed externally through the Firewall to FTP servers within The DES trusted network. FTP servers in the DMZ will be allowed. FTP clients on the inside will be configured to use FTP Passive Mode and will not use FTP Normal Mode. This does not include selected access via a VPN to a selected internal resource such as DDD is doing with their external providers.
Telnet	Yes	No	No	No	Telnet access will be allowed from the inside network to the outside network. For telnet from the outside to the inside network, authorization by ISA is required.
TN3270	Yes	No	No	No	TN3270 access will be allowed from the inside network to the outside network. Access from outside to inside will be restricted to the specific subnets requiring access to mainframe applications. This service should be closed and this access only provided inbound via a VPN, Citrix Secure Gateway, or SSL (Host on Demand, WebConnect, et al.
Rlogin	No	No	No	No	Rlogin to DES hosts from external networks requires written approval from the DSO and the use of strong authentication.

HTTP	Yes	No	Yes	No	All WWW servers intended for access by external users will be hosted outside the DES firewall. No inbound HTTP will be allowed through the DES firewall unless it uses reverse proxy and strong encryption/authentication (e.g. SSL).
SSL	Yes	No	Yes	Yes	Secure Sockets Layer sessions using client side certificates is required when SSL sessions are to be passed through the DES firewall.
POP3/IMAP	No	No	No	No	DES will not use the POP3/IMAP protocol for mail services. However, specific cases will be considered if a business requirement can be shown. As of April, 2003, a limited UNIX presence in the DERS Sun system exists.
NNTP	Yes	No	No	No	No external access will be allowed to the NNTP server.
Streaming Audio and Video	No	No	No	No	Department policy specifically denies the use of the Internet as a radio or music player. Due to its bandwidth requirements streaming video by default will be denied. However, specific cases will be considered if a business requirement can be shown.
Lp	No	No	No	No	Inbound Lp services are to be disabled at the DES firewall.
finger	No	No	No	No	Inbound finger services are to be disabled at the DES firewall.
gopher	No	No	No	No	Inbound gopher services are to be disabled at the DES firewall.
whois	No	No	No	No	Inbound whois services are to be disabled at the DES firewall.
SQL	No	No	No	No	Direct connections from external hosts to internal databases are not allowed. The use of reverse proxy will be considered by the SWG on a case by case basis.
Rsh	No	No	No	No	Inbound rsh services are to be disabled at the DES firewall.
Citrix	Yes	No	No	Yes	Requires Secure Gateway or a VPN.
RDP	Yes	No	No	Yes	Requires Secure Gateway or a VPN.
Other, such as NFS	No	No	No	No	Access to any other service not mentioned above will be denied in both directions.

[1] Status (Y/N) = whether users can use the service

[2] Auth (Y/N) = whether any form of authentication (strong or otherwise) is performed before the service can be used